UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/784,512	02/14/2001	David C. Platt	TIVO0067	3300

29989 7590 03/09/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/784,512	PLATT, DAVID C.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 26 have been presented for examination. Claims 1 – 3, 5, 8, 10 – 14, 17, 18 20 – 22, 25 and 26 have been amended in an amendment filed 12/20/2004.

Response to Arguments

2. As per claim 25, Applicant remarks "Daniel does not teach a system that denies access to unauthorized machines". Examiner notes Applicant's arguments have been fully considered but are not persuasive because Daniel teaches "the Interactive Online Database System IODS discriminates and limits accessibility of the individual terminals to the data stored within the IODS" (Daniel: see for example, Column 8 Line 35 – 36 and Column 8 Line 4 – 6).

3. As per claim 10, Applicant remarks "Mankoff does not teach a unique encrypted coupon authentication number for each receiving device that is used as a coupon key to validate coupons". Examiner notes (I) Applicant's arguments have been fully considered but are not persuasive because a coupon key is merely interpreted as a unique ID used for authentication purpose and Mankoff teaches (a) "the encrypted coupon authentication number is downloaded from the network to the PC or PDA over a secure link" (Mankoff: see for example, Column 5 Line 34 – 37) and (b) "when the user desires to redeem the virtual coupon, the coupon is first authenticated before it is honored" (Mankoff: see for example, Column 5 Line 41 – 43). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

For additional arguments to claim 10, Examiner notes (II) Applicant's arguments have been fully considered – please see the corresponding new ground rejection in following 2nd Non-Final office action.

4. As per claim 13, 17 and 18, Applicant asserts "Mankoff does not teach a system that provides a coupon authentication number that is unique to a receiving device and the unique coupon authentication number is used to perform a hash operation on an offer ID number to generate a coupon ID number". However, Applicant's arguments have been fully considered – please see the corresponding new ground rejection in following 2nd Non-Final office action.

5. As per claim 26, Applicant remarks "Daniel does not teach a new random coupon authentication number for each receiving device that is unique for each receiving device and wherein said coupon authentication number is used to authenticate coupon on each receiving device". Examiner notes Applicant's arguments have been fully considered but are not persuasive because Daniel teaches auditing and reducing the security risk from any couple anomalies by isolating the cause of the fraud (Daniel: see for example, Column 12 Line 12 – 22 and Figure 4 Element 64) and thereby it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate the new coupon numbers to replace the old ones that have been detected with the frauds as taught by Daniel.

Claim Rejections - 35 USC § 102

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim 25 is rejected under 35 U.S.C. 102(e) as being anticipated by Daniel (Patent Number: US 6766301 B1), hereinafter referred to as Daniel.

As per claim 25, Daniel teaches a method for preventing security leak of authentication number database, comprising the steps of:

keeping said authentication number database behind a firewall (Daniel: see for example, Column 4 Line 62 – 66, Column 8 Line 45 – 47 and Figure 1 Element 7); and

denying access to unauthorized machines (Daniel: see for example, Figure 6 Element 88, Column 8 Line 35 – 36 and Column 8 Line 4 – 6).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 – 16 and 18 – 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (Patent Number: 2001/0014868), hereinafter referred to as Herz, in view of Chen (Patent Number: 5602918), hereinafter referred to as Chen.

As per claim 10, Herz teaches a method for generating a coupon authentication number for each receiving device coupled to a coupon distribution system, comprising the steps of:

activating at least one receiving device (Herz: see for example, Figure 1 Element 131 – 13"n");

generating a unique coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly generated and can be of any length of bits long (Herz: see for example, Paragraph [0282]);

storing said coupon authentication number in a coupon authentication number database (Herz: see for example, Figure 1 Element 122 & Paragraph [0022]);

Herz teaches implementing encryption of a coupon (Herz: see for example, Paragraph [0287]). However, Herz does not disclose expressly communicating said coupon authentication number to a key server; encrypting said coupon authentication number at said key server.

Chen teaches communicating said coupon authentication number to a key server; encrypting said coupon authentication number at said key server (Chen: see for

example, Column 5 Line 50 – 56: Chen teaches the use of partially digital signing by the key server known as "coupon generation").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Herz because Chen teaches providing a mechanism to enable parties on an unsecure network to exchange authenticatable data using a key server to minimize the complexity and hardware requirements of the system (Chen: see for example, Column 36 – 41 and Column 6 Line 47 – 48).

sending said encrypted coupon authentication number from said key server to a receiving device which saves said encrypted coupon authentication number as a coupon key to be used to validate coupons (Herz: see for example, Paragraph [0288]: a coupon key is merely interpreted as a unique ID used for authentication purpose).

As per claim 2, claim 2 is similar to claim 10. Therefore, see same rationale addressed above in rejecting claim 10.

As per claim 3 and 11, Herz in view of Chen teaches the claimed invention as described above (see claim 2 and 10 respectively). Herz further teaches step of encrypting said coupon authentication number is performed by said key server using said receiving device's public key which is stored both in said activation database and said receiving device's persistent storing device (Herz: see for example, Paragraph [0285] and Paragraph [0288]: Herz teaches using appropriate encryption scheme for the

signature (e.g. PGP) – public key is one of the commonly used ciphering algorithms by PGP. Herz also teaches assigning a public key to the person who may use the coupon to prevent transferability Paragraph [0285] and the terminal devices (e.g. personal computers) must have a hard-drive to store the public key and the activation database must also store the public key to validate the coupon number associated with the receiving device in order to prevent transferability Paragraph [0285]).

As per claim 4 and 12, Herz in view of Chen teaches the claimed invention as described above (see claim 2 and 10 respectively). Herz in view of Chen further teaches embedding a date or time stamp in said coupon key for convenience to replace said authentication number when ever said authentication number database is compromised (Herz: see for example, Paragraph [0282] – [0285] and Paragraph [0287] Line 1 – 6: Herz teaches the coupon also includes Expiration Date (which has a date or time stamp) besides the unique coupon number and one unique identifier is sufficient to retrieve the remaining fields (Herz: see for example, Paragraph [0287] Line 1 – 6); thereby, it is evident to replace said authentication number when ever said authentication number database is compromised).

As per claim 5, claim 5 is similar to claim 18. Therefore, see same rationale addressed above in rejecting claim 18.

As per claim 6 and 14, Herz in view of Chen teaches the claimed invention as described above (see claim 5 and 13 respectively). Herz further teaches confirming a unique offer ID number for said coupon comprises the sub-steps of:

checking whether or not said client has designated a unique offer ID number for said coupon (Herz: see for example, Paragraph [0038], [0283] and [0288]);

wherein if said client has designated a unique offer ID number for said coupon, checking the uniqueness of said offer ID number and resolving possible collisions with other offers (Herz: see for example, Paragraph [0288] Item (1) & (2)); and

wherein if said client has not designated a unique offer ID number for said coupon, generating a unique offer ID number for said coupon (This is evidently one of the design choice for the purpose of the coupon if this particular coupon is not rejected or cancelled).

As per claims 7, 15 and 23, Herz in view of Chen teaches the claimed invention as described above (see claims 5, 13 and 18 respectively). Herz further teaches offer ID number is implemented as ASCII character strings (The format of a number is always transformable between different types).

As per claims 8, 16 and 24, Herz in view of Chen teaches the claimed invention as described above (see claims 5, 13 and 18 respectively). Herz further teaches N is 6 (Six as the number of characters is one of the design choices commonly used for an identification code that can also provide proper security).

As per claim 9, claim 9 is similar to the claim 17. Therefore, see same rationale addressed above in rejecting claim 17.

As per claim 18, Herz teaches a system for coupon encryption, distribution, and validation, comprising:

a client which issues coupons, each of said coupons is designated a unique offer ID number (Herz: see for example, Paragraph [0283] and [0038]);

an information service center which comprises an activation database, a coupon authentication number database, and a key server (Herz: see for example, Figure 1 Element 122 & Paragraph [0022]);

Herz does not disclose expressly a key server.

Chen teaches a key server (Chen: see for example, Column 5 Line 50 – 56: Chen teaches the use of partially digital signing by the key server known as "coupon generation").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Herz because Chen teaches providing a mechanism to enable parties on an unsecure network to exchange authenticatable data using a key server to minimize the complexity and hardware requirements of the system (Chen: see for example, Column 36 – 41 and Column 6 Line 47 – 48).

a plurality of service receiving devices, each of which is coupled to a displaying device (Herz: see for example, Paragraph [0290]);

a channel through which said information service center and a service receiving device communicate (Herz: see for example, Figure 1 Element 103);

wherein said information service center generates a unique coupon authentication number for each said service receiving device, wherein said coupon authentication number is stored in said coupon authentication number database and is communicated to said key server (Herz: see for example, Paragraph [0282] and [0287]);

wherein said key server encrypts said coupon authentication number using an encryption algorithm and sends encrypted authentication number to said service receiving device (Herz: see for example, Paragraph [0287]);

wherein said service receiving device comprises a crypto-chip and a hard drive (Herz: see for example, Paragraph [0285], [0288] and [0290]: Herz teaches assigning a public key to the person who may use the coupon to prevent transferability Paragraph [0285] and the terminal devices (e.g. personal computers) must have a hard-drive. Herz also teaches customer may use smart card (with crypto-chip) during the coupon process and smart card must have private keys associated with the users / receiving devices).

wherein said crypto-chip performs a hash operation on said offer ID number using said encrypted coupon authentication number and takes the first or last N digits of the hashed result as a coupon ID number for said coupon (Herz: see for example, Paragraph [0282] – [0287] and [0038]: Herz teaches using hash function to sign the

coupon, which indeed includes (a) said offer ID number and (b) the coupon authentication number. Since the offer ID number is the product related information, which is the public information, the hash key must use the coupon authentication number as the private secret information); and

wherein said coupon may be validated by said key server, which uses said service receiving device's serial number to look up the unencrypted coupon authentication number stored in said coupon authentication number database and performs a hash operation on said offer ID number using said unencrypted coupon authentication number and compares a base number taken from the first or last N digits of the hashed result with said coupon ID number submitted, and validates said coupon if said base number and said coupon number match (Herz: see for example, Paragraph [0288] and [0287]: Herz teaches the receiving device's public key is the customer identified in the coupon).

As per claim 1, claim 1 does not further teach over claim 18 except that Herz further teaches, in claim 1, said receiving device comprises a persistent storage device which stores one or more public keys assigned to said receiving device, and a crypto-chip which stores one or more private keys assigned to said receiving device Herz: see for example, Paragraph [0285], [0288] and [0290]: Herz teaches assigning a public key to the person who may use the coupon to prevent transferability Paragraph [0285] and the terminal devices (e.g. personal computers) must have a hard-drive. Herz also

teaches customer may use smart card (with crypto-chip) during the coupon process and smart card must have private keys associated with the users / receiving devices).

As per claim 13, claim 13 is similar to claim 18; besides that, in further regards to claim 13, Herz further teaches displaying detailed instructions about how to redeem said coupon (Herz: see for example, Paragraph [0281]: Internet must provide information how to use / obtain the coupon / rebate).

As per claim 19, Herz in view of Chen teaches the claimed invention as described above (see claim 18). Herz further teaches receiving device is a personal video recorder and said displaying device is a TV set (Herz: see for example, Paragraph [0021]: Herz teaches the secured terminal device can be any terminal device adapted for use with any type of network connections).

As per claim 20 Herz in view of Chen teaches the claimed invention as described above (see claim 18). Herz further teaches channel can be a telephone modem, or a cable modem, or a local area network (Herz: see for example, Paragraph [0021]).

As per claim 21, Herz in view of Chen teaches the claimed invention as described above (see claim 18). Herz further teaches coupon authentication number is randomly generated and can be of any length of bits (random number is widely used in the field to enhance the security).

As per claim 22, Herz in view of Chen teaches the claimed invention as described above (see claim 18). Herz further teaches offer ID number is randomly generated and can be of any length of bits (random number is widely used in the field to enhance the security).

As per claim 23, Herz in view of Chen teaches the claimed invention as described above (see claims 18). Herz further teaches offer ID number is implemented as ASCII character strings (The format of a number is always transformable between different types).

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Herz (Patent Number: 2001/0014868), hereinafter referred to as Herz, in view of Chen (Patent Number: 5602918), hereinafter referred to as Chen, and in view of Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff.

As per claim 17, Herz teaches a method for validating said cryptographic coupon, comprising the steps of:

submitting said offer ID number (Herz: see for example, Paragraph [00283]), said receiving device's serial number (Herz: see for example, Paragraph [00285] & [0288]: This is used to match the coupon number with the associated customer), and said coupon ID number (Herz: see for example, Paragraph [00282]) to a vendor by the user who accepted said coupon);

entering said offer ID number, said receiving device's serial number, and said coupon ID number by said vendor who accesses to a common gateway interface at said service center (Herz: see for example, Paragraph [00282] – [0288]). However, Herz does not disclose expressly accessing to a common gateway interface at said service center.

Mankoff teaches accessing to a common gateway interface (CGI) at said service center (Mankoff: see for example, Column 3 Line 8).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Mankoff within the system of Daniel because Mankoff teaches providing an improved method for electronically delivery and use of coupons (Mankoff: see for example, Column 1 Line 36 – 37).

Herz further teaches checking the unencrypted authentication number from said coupon authentication number database (Herz: see for example, Paragraph [0288]). However, Herz in view of Mankoff does not disclose expressly using a key server to obtain the unencrypted authentication number.

Chen teaches using a key server to obtain the unencrypted authentication number (Chen: see for example, Column 5 Line 50 – 56: Chen teaches the use of partially digital signing by the key server known as "coupon generation").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Herz in view of Mankoff because Chen teaches providing a mechanism to enable parties on an unsecure network to exchange authenticatable data using a key server to minimize the

complexity and hardware requirements of the system (Chen: see for example, Column 36 – 41 and Column 6 Line 47 – 48).

Accordingly, Herz in view of Mankoff teaches checking, by said key server, the unencrypted authentication number from said coupon authentication number database.

Herz further teaches:

performing a hash operation on said offer ID number using said unencrypted authentication number as a key (Herz: see for example, Paragraph [0282] – [0287] and [0038]: Herz teaches using hash function to sign the coupon, which indeed includes (a) said offer ID number and (b) the coupon authentication number. Since the offer ID number is the product related information, which is the public information, the hash key must use the coupon authentication number as the private secret information).

taking the first N digits of the hashed result and comparing this N-digit number with said coupon ID number submitted by the user; and validating said coupon if said N-digit number matches with said coupon ID number (Herz: see for example, Paragraph [0287] and [0288]).

9. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniel (Patent Number: US 6766301 B1), hereinafter referred to as Daniel, in view of Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff.

As per claim 26, Daniel teaches a method for remedying security leak of authentication number database, comprising the steps of: fixing said security leak;

generating a new random coupon authentication number for each receiving device that is unique for each receiving device (Daniel: see for example, Column 12 Line 13 – 22 and Figure 4 Element 64: Tracing and reducing the fraud after any couple anomalies as taught by Daniel is one type of fixing said security leak: Daniel teaches auditing and reducing the security risk from any couple anomalies by isolating the cause of the fraud and thereby it would have been obvious to a person of ordinary skill in the art at the time the invention was made to recognize generating the new coupon numbers to replace the old ones that have been detected with the frauds);

Daniel does not disclose expressly wherein said coupon authentication number is used to authenticate coupons on each receiving device.

Mankoff teaches said coupon authentication number is used to authenticate coupons on each receiving device (Mankoff: see for example, Column 5 Line 36 – 39).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Mankoff within the system of Daniel because Mankoff teaches providing an improved method for electronically delivery and use of coupons (Mankoff: see for example, Column 1 Line 36 – 37).

Mankoff further teaches distributing said coupon authentication number to each receiving device via a key server (Mankoff: see for example, Column 5 Line 34 – 37).

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff, in view of Chen (Patent Number: 5602918), hereinafter referred to as Chen.

As per claim 10, Mankoff teaches a method for generating a coupon authentication number for each receiving device coupled to a coupon distribution system, comprising the steps of:

activating at least one receiving device (Mankoff: see for example, Column 3 Line 53 – 54, Column 5 Line 61 – 67 and Column 5 Line 26 – 46);

generating a unique coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly generated and can be of any length of bits long (Mankoff: see for example, Column 5 Line 31);

storing said coupon authentication number in a coupon authentication number database (Mankoff: see for example, Figure 1 Element 27, Column 3 Line 50 – 54 and Column 2 Line 15 – 17);

Herz teaches implementing encryption of a coupon (Mankoff: see for example, Column 5 Line 35 – 37). However, Herz does not disclose expressly communicating said coupon authentication number to a key server; encrypting said coupon authentication number at said key server.

Chen teaches communicating said coupon authentication number to a key server; encrypting said coupon authentication number at said key server (Chen: see for example, Column 5 Line 50 – 56: Chen teaches the use of partially digital signing by the key server known as "coupon generation").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Herz

because Chen teaches providing a mechanism to enable parties on an unsecure network to exchange authenticatable data using a key server to minimize the complexity and hardware requirements of the system (Chen: see for example, Column 36 – 41 and Column 6 Line 47 – 48).

sending said encrypted coupon authentication number from said key server to a receiving device which saves said encrypted coupon authentication number as a coupon key to be used to validate coupons (Mankoff: see for example, Column 5 Line 35 – 37: a coupon key is merely interpreted as a unique ID used for authentication purpose).

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Gressel (Patent Number: 5852665), discloses crypto-chip for smart card.

b. Freeman (Patent Number: US 6450407 B1), disclose coupon offer ID number for product families.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100